CLAIMS

What is claimed is:

1. A method of establishing a secure communication channel between a first network device and a second network device that controls the first network device, comprising:

receiving, at the second network device, at least one authentication certificate from the first network device, wherein the at least one authentication certificate includes an authentication key;

searching a data store associated with the second network device for an authentication certificate that matches the at least one authentication certificate received from the first network device;

if the data store includes a matching authentication certificate, then implementing a secure communication channel using information derived from the matching authentication certificate; and

if the data store does not include a matching authentication certificate, then:

computing a master secret from information associated with the at least one authentication certificate received from the first network device; and

implementing a secure communication channel using information derived from the new master secret.

2. The method of claim 1, wherein the at least one authentication certificate comprises an X.509 certificate.

3. The method of claim 1, further comprising:

transmitting from the second network device to the first network device an introductory message including a first session identifier and a list of one or more cipher suites; and

receiving at the second device, a response to the introductory message, wherein the response includes a second session identifier and an indicator identifying a selected cipher suite.

4. The method of claim 3, further comprising implementing a secure communication channel using the first session identifier if the first session identifier matches the second session identifier.

5. The method of claim 1, wherein computing a master secret from information associated with the at least one authentication certificate received from the first network device comprises verifying the authentication certificate received from the first network device using the authentication key.

6. A method of adding a device to a UPnP network, comprising:

retrieving, at a control point in the UPnP network, a device description associated with the UPnP device;

invoking, at the control point, a first authentication process to authenticate the device with the control point;

retrieving, at the control point, a service description associated with the device; and

retrieving, at the control point, a presentation page associated with the device.

7. The method of claim 6, wherein upon connection to the UPnP network the device multicasts information about itself to a predetermined address.

8. The method of claim 7, wherein the control point uses the information multicast by the device to retrieve the device description.

9. The method of claim 6, wherein the first authentication process comprises:

receiving a certificate from the device; and

authenticating the device using the certificate.

10. The method of claim 9, wherein the first authentication process further comprises:

sending a certificate from the control point to the device; and

using the certificate at the device to authenticate the control point with the device.

11. The method of claim 9, wherein the certificate includes a public key associated with the device.

12. The method of claim 9, wherein the certificate is issued by a certificate authority and includes a public key associated with the certificate authority.

13. The method of claim 10, wherein sending the certificate from the control point to the device comprises:

loading the certificate onto a memory module; and

transferring the certificate from the control point to the device on the memory module.

14. The method of claim 6, wherein the device invokes a second authentication process to authenticate the control point with the device.

15. The method of claim 14, wherein the second authentication process comprises transmitting a PIN/password from the control point to the device.

16. The method of claim 15, wherein the PIN/password comprises:

a credential; and

a hash of a certificate sent from the device to the control point.

17. A method of adding a control point to a UPnP network, comprising:

transmitting a search request multicast from the control point to a predetermined network address;

receiving a response to the multicast from at least one device in the UPnP network, wherein the response includes an indicator requesting a secure communication between the device and the control point;

invoking, at the control point, a first authentication process to authenticate the device with the control point;

retrieving, at the control point, a device description associated with the UPnP device

retrieving, at the control point, a service description associated with the device; and

retrieving, at the control point, a presentation page associated with the device.

18. The method of claim 17, wherein the first authentication process comprises:

receiving a certificate from the device; and

authenticating the device using the certificate.

19. The method of claim 18, wherein the first authentication process further comprises:

sending a certificate from the control point to the device; and

using the certificate at the device to authenticate the control point with the device.

20. The method of claim 18, wherein the certificate includes a public key associated with the device.

21. The method of claim 18, wherein the certificate is issued by a certificate authority and includes a public key associated with the certificate authority.

22. The method of claim 19, wherein sending the certificate from the control point to the device comprises:

loading the certificate onto a memory module; and

transferring the certificate from the control point to the device on the memory module.

23. The method of claim 17, wherein the device invokes a second authentication process to authenticate the control point with the device.

24. The method of claim 20, wherein the second authentication process comprises transmitting a PIN/password from the control point to the device.

25. The method of claim 21, wherein the PIN/password comprises:

a credential; and

a hash of a certificate sent from the device to the control point.